(g) Security of automated systems is governed by AR 380–19. Provost marshals using automated systems will appoint, in writing, an Information Assurance Security Officer (IASO) who will ensure implementation of automation security requirements within the organization. Passwords used to control systems access will be generated, issued, and controlled by the IASO.

(h) Supervisors at all levels will ensure that personnel whose duties involve preparation, processing, filing, and release of military police records are knowledgeable of and comply with policies and procedures contained in this part, AR 25–55, AR 340–21, and other applicable HQDA directives. Particular attention will be directed to provisions on the release of information and protection of privacy.

(i) Military police records identifying juveniles as offenders will be clearly marked as juvenile records and will be kept secure from unauthorized access by individuals. Juvenile records may be stored with adult records but clearly designated as juvenile records even after the individual becomes of legal age. In distributing information on juveniles, provost marshals will ensure that only individuals with a clear reason to know the identity of a juvenile are provided the identifying information on the juvenile. For example, a community commander is authorized to receive pertinent information on juveniles. When a MPR identifying juvenile offenders must be provided to multiple commanders or supervisors, the provost marshal must sanitize each report to withhold juvenile information not pertaining to that commander's area of responsibility.

(j) Military police records in the custody of USACRC will be processed, stored and maintained in accordance with policy established by the Director, USACRC.

§ 635.2 Safeguarding official information.

(a) Military police records are unclassified except when they contain national security information as defined in AR 380–5.

(b) When military police records containing personal information transmitted outside the installation law enforcement community to other departments and agencies within DOD, such records will be marked ''For Official Use Only.'' Records marked ''For Official Use Only'' will be transmitted as prescribed by AR 25–55. Use of an expanded marking is required for certain records transmitted outside DOD per AR 25–55.

(c) Military police records may also be released to Federal, state, local or foreign law enforcement agencies as prescribed by AR 340–21. Expanded markings will be applied to these records.

§ 635.3 Special requirements of the Privacy Act of 1974.

(a) Certain personal information is protected under the Privacy Act and AR 340–21.

(b) Individuals requested to furnish personal information must normally be advised of the purpose for which the information is routinely used.

(c) Army law enforcement personnel performing official duties often require an individual's SSN for identification purposes. Personal information may be obtained from identification documents without violating an individual's privacy and without providing a Privacy Act Statement. This personal information can be used to complete military police reports and records. The following procedures may be used to obtain SSNs:

(1) Active Army, U.S. Army Reserve (USAR), Army National Guard (ARNG) and retired military personnel are required to produce their DD Form 2A (Act), DD Form 2 (Act), DD Form 2 (Res), or DD Form 2 (Ret) (U.S. Armed Forces of the United States General Convention Identification Card), or other government issued identification, as appropriate.

(2) Family members of sponsors may be requested to produce their DD Form 1173 (Uniformed Services Identification and Privilege Card). Information contained thereon (for example, the sponsor's SSN) may be used to verify and complete applicable sections of MPRs and related forms.

(3) DOD civilian personnel may be requested to produce their appropriate service identification. DA Form 1602

(Civilian Identification) may be requested from DA civilian employees. If unable to produce such identification, DOD civilians may be requested to provide other verifying documentation.

(4) Non-DOD civilians, including family members and those whose status is unknown, will be advised of the provisions of the Privacy Act Statement when requested to disclose their SSN.

(d) Requests for new systems of military police records, changes to existing systems, and continuation systems, not addressed in existing public notices will be processed as prescribed in AR 340–21, after approval is granted by HQDA, OPMG (DAPM–MPD–LE).

§ 635.4 Administration of expelled or barred persons file.

(a) When action is completed by an installation commander to bar an individual from the installation under 18 U.S.C. 1382 the installation provost marshal will be provided—

(1) A copy of the letter or order barring the individual.

(2) Reasons for the bar.

(3) Effective date of the bar and period covered.

(b) The provost marshal will maintain a list of barred or expelled persons. When the bar or expulsion action is predicated on information contained in military police investigative records, the bar or expulsion document will reference the appropriate military police record or MPR. When a MPR results in the issuance of a bar letter the provost marshal will forward a copy of the bar letter to Director, USACRC to be filed with the original MPR. The record of the bar will also be entered into COPS, in the Vehicle Registration module, under Barrings.

§ 635.5 Police intelligence/criminal information.

(a) The purpose of gathering police intelligence is to identify individuals or groups of individuals in an effort to anticipate, prevent, or monitor possible criminal activity. If police intelligence is developed to the point where it factually establishes a criminal offense, an investigation by the military police, U.S. Army Criminal Investigation Command (USACIDC) or other investigative agency will be initiated.

(b) Information on persons and organizations not affiliated with DOD may not normally be acquired, reported, processed or stored. Situations justifying acquisition of this information include, but are not limited to—

(1) Theft, destruction, or sabotage of weapons, ammunition, equipment facilities, or records belonging to DOD units or installations.

(2) Possible compromise of classified defense information by unauthorized disclosure or espionage.

(3) Subversion of loyalty, discipline, or morale of DA military or civilian personnel by actively encouraging violation of laws, disobedience of lawful orders and regulations, or disruption of military activities.

(4) Protection of Army installations and activities from potential threat.

(5) Information received from the FBI, state, local, or international law enforcement agencies which directly pertain to the law enforcement mission and activity of the installation provost marshal office, MACOM provost marshal office, or that has a clearly identifiable military purpose and connection. A determination that specific information may not be collected, retained or disseminated by intelligence activities does not indicate that the information is automatically eligible for collection, retention, or dissemination under the provisions of this part. The policies in this section are not intended and will not be used to circumvent any federal law that restricts gathering, retaining or dissemination of information on private individuals or organizations.

(c) Retention and disposition of information on non-DOD affiliated individuals and organizations are subject to the provisions of AR 380–13 and AR 25–400–2.

(d) Police intelligence will be actively exchanged between DOD law enforcement agencies, military police, USACIDC, local, state, federal, and international law enforcement agencies. One tool developed by DOD for sharing police intelligence is the Joint Protection Enterprise Network (JPEN). JPEN provides users with the ability to post, retrieve, filter, and analyze real-world events. There are seven reporting criteria for JPEN:

(1) Non-specific threats;